Roberto Flor, Daniela Falcinelli, Stefano Marcolini, *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet*, DIPLAP Editor, Milano, 2015

LA GIUSTIZIA PENALE NELLA RETE? TUTELA DELLA RISERVATEZZA *VERSUS* INTERESSE ALL'ACCERTAMENTO E ALLA PREVENZIONE DEI REATI NELLA RECENTE GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

Roberto Flor

1. Introduzione

Il *cyberspace* viene oggi descritto come un "*wild west*" della globalizzazione del crimine [1]. Ad esso vengono legate diverse espressioni metaforiche, non tutte immediatamente comprensibili, quali: "tecnologia veloce dei flussi informativi globali" e delle "traslazioni" "uomo-macchina" attraverso la rete; "sfera di iper-mobilità che riflette la pace globale della iper-modernità"; tecnologia "*open-ended*", decentralizzata e non gerarchica; "connessione con la realtà virtuale"; "topografia" virtuale creata dalla rete quale sistema di interattività e multimedialità. Esse evocano, però, il superamento della concezione meramente "tecnica" di Internet e del *cyberspace* - ossia quali reti o spazi globali di interconnessione di *computers* - per abbracciare una dimensione sociologica, basata sulla loro forza riconfigurativa della società e delle esperienze personali degli utenti, influenzate in modo determinante dai nuovi modi di comunicazione dinamica, transnazionale ed interattiva[2].

Oggi il *cyberspace* costituisce uno spazio virtuale in continua evoluzione che consente non solo la delocalizzazione delle risorse, anche grazie alle nuova dimensione

[1] Vedi B. SANDYWELL, *On the globalisation of crime: the Internet and new criminality*, in Y. JEWKES, M. YAR, *Handbook of Internet Crime*, Willan Publishing, 2010, 38 e ss. Cfr., inoltre, R. FLOR, *La tutela penale della proprietà intellettuale ed il contrasto alla commercializzazione ed alla circolazione in Internet di opere o prodotti con segni falsi o alterati*, in L. CAMALDO (cur.), *La circolazione e il contrabbando di prodotti contraffatti o pericolosi. La tutela degli interessi finanziari dell'Unione Europea e la protezione dei consumatori* , Torino , G. Giappichelli - Torino , 2013 , 118 - 178

[2] Cfr. T. JORDAN, *Cyberpower: A Sociology and Politics of Cyberspace and the Internet*, Londra, 1998; D. Lyon, *The Electronic Eye: The Rise of Surveillance Society*, Cambridge, 1994; B. SANDYWELL, *Monsters in Cyberspace: Cyberphobia and Cultural Panic in the Information Age*, in *Inf. Com. Soc*., 9, 1, 39-61. Alcuni Autori parlano di effettivo impatto sociale del *cyberspace*: vedi D.S. WALL, *Cybercrimes: New Wine, no Bottles*?, ora in D. S. WALL, *Cyberspace Crime*, Ashgate Publishing, 2003, 3 e ss. Sugli elementi specializzanti del *cyberspace* rispetto al mondo fisico vedi C. REED, *Making Laws for Cyberspace*, Oxford, 2012, 25 e ss.

del *cloud*[3] e della "struttura" del *web*, ma altresì la detemporalizzazione delle attività, che possono essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente, che fanno venire meno l'esigenza di un "collegamento" o "contatto" fisico fra persona e sistema informatico.

"Smaterializzazione" e "velocizzazione" coinvolgono, dunque, anche le condotte concrete, che prescindono o si distanziano dalla fisicità dei comportamenti o dei fatti esteriori capaci di "incorporare" l'accadimento materiale (il danno o il pericolo concreto)[4].

L'innovazione-rivoluzione tecnologica offre però anche nuovi strumenti e mezzi per la ricerca delle prove, e consente di perseguire altresì fini "preventivi". La concreta esigenza di misure efficaci di contrasto a gravi forme di criminalità vale anche rispetto a reati "tradizionali", che trovano nelle nuove tecnologie un essenziale ausilio per la loro realizzazione. Si pensi solo alle attività preparatorie di attentati terroristici, che possono trovare in Internet un formidabile mezzo di comunicazione e di pianificazione degli attacchi, oppure alla lotta contro la diffusione di materiale pedopornografico *online*.

In questo contesto la sentenza del 13 maggio 2014 della Corte di Giustizia sul c.d. caso Google/Spagna è immediatamente passata alle cronache come la decisione che ha riconosciuto il c.d. "diritto all'oblio"[5].

In verità la controversia, sul piano sociale prima ancora che su quello del diritto penale sostanziale, e rilevante per tutto il sistema di giustizia penale, risulta essere più complessa, in quanto coinvolge questioni attinenti non solo ai possibili profili di responsabilità del fornitore di un servizio nella società dell'informazione e di Internet, ai limiti degli "ordini" delle "autorità competenti" di rimozione di dati e informazioni per la tutela della riservatezza in rapporto al bilanciamento con gli altri diritti fondamentali coinvolti ed il perseguimento di interessi di rilevanza collettiva, ma anche ai profili distopici che talvolta si vogliono attribuire a Internet, proprio quale *"wild west*" della globalizzazione del crimine, portato a estremi apocalittici.

Non è certo la prima volta che la Corte di Giustizia ha dovuto affrontare problematiche riguardanti proprio il bilanciamento fra le diverse esigenze, da un lato, di tutela dei diritti fondamentali e, dall'altro, di accertamento e prevenzione di attività illecite e di reati[6]. Pur trattandosi, in questi ultimi casi, di questioni pregiudiziali sull'interpretazione delle direttive 2000/31/CE sul commercio elettronico, 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, 2004/48/CE sul rispetto dei diritti di proprietà intellettuale,

[3] La nozione di *cloud computing* allude ad un insieme di tecnologie che permettono di memorizzare, archiviare e/o elaborare dati grazie all'utilizzo di risorse hardware/software delocalizzate in rete. Cfr., per una spiegazione tecnica, B. FURHT, A. ESCALANTE, *Handbook of Cloud Computing*, Lexis Nexis, 2010.

[4] Cfr. quanto già evidenziato da L. PICOTTI, *Sicurezza, informatica e diritto penale*, in M. DONINI, M. PAVARINI (cur.), *Sicurezza e diritto penale*, Bologna, 2011, 217 e ss., 223-224.

[5] Corte di Giustizia dell'Unione europea, sent. 13 maggio 2014 (C-131/12). Per i primi commenti si rinvia a B. VAN ALSENOY, A. KUCZERAWY AND J. AUSLOOS, *Search engines after Google Spain: internet@liberty or privacy@peril?*, in ICRI, 15/2013, 1-74; G. FINOCCHIARO, *Editoriale*, in *Giustizia civile.com*, 2014, 3 e ss.; A. PALMIERI, R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quaderni del Foro Italiano*, 1, 2014, 1-16.

[6] Vedi, ad esempio, Corte di Giustizia dell'Unione europea, sent. 24 novembre 2011 (C-70/10) e 16 febbraio 2012 (C -360/10), nonché, in termini parzialmente diversi, Corte di Giustizia dell'Unione europea, sent. 27 marzo 2014 (C-314/12). Cfr. ampiamente R. FLOR, *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale*?, in *Dir. inf*., 2014, 775 – 803.

95/46/CE sul trattamento dei dati personali e 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, esse hanno, di fatto, posto in discussione l'uso di taluni mezzi tecnologici "invasivi" rispetto alla tutela dei diritti fondamentali, ferma restando la validità degli atti europei.

Con la sentenza del 13 maggio 2014 (c.d. caso Google/Spagna), invece, la Corte di Giustizia ha affermato la prevalenza dei diritti tutelati dagli artt. 7 e 8 della Carta, in determinate condizioni, rispetto alla libertà di espressione e agli interessi economici dei *providers,* rafforzando in questo modo la posizione giuridica della persona interessata da un trattamento di dati personali, benchè non sia pacifico poter ricavare dalle norme della direttiva 95/46, intepretate alla luce delle disposizioni dalla Carta, un diritto "generalizzato" all'oblio.[7]

Questa sentenza giunge dopo un'altra importante decisione (c.d. caso *data retention*) [8], in cui i Giudici di Lussemburgo hanno affrontato per la prima volta la delicata questione concernente il bilanciamento fra le esigenze di repressione ed accertamento dei reati e la tutela dei diritti fondamentali dell'individuo, che possono essere fortemente limitati dagli obblighi di conservazione dei dati di traffico telefonico e telematico nella società informazione, annullando la direttiva 2006/24 perché contraria agli artt. *7,* 8 e 11 della Carta dei diritti fondamentali dell'Unione europea. In quest'ultima sentenza la Corte ha esaminato gli obblighi di conservazione dei dati nell'UE alla luce dei principi di necessità e proporzionalità, tenuto conto e nell'interesse della sicurezza nazionale, del buon funzionamento del mercato interno e del rafforzamento del rispetto della vita privata, nonché del diritto fondamentale alla protezione dei dati personali, fornendo alcune linee guida essenziali, che si inseriscono inevitabilmente nel contesto più ampio della riforma in atto, a livello europeo, di tutta la disciplina in materia di tutela della *privacy,* attraverso un *corpus* unico di norme[9].

Queste ultime due decisioni, in particolare, se da un lato rafforzano la tutela della riservatezza, dall'altro segnano uno strappo epocale nell'odierna società di Internet, ponendo dei limiti decisi all'uso delle tecnologie e della rete, che non sempre possono produrre effetti positivi rispetto alla tutela di rilevanti contro interessi di natura generale e collettiva.

2. Le principali linee argomentative della Corte di Giustizia nel caso Google/Spagna

In estrema sintesi, nel c.d. caso Google/Spagna[10] la Corte ha affermato che l'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di

[7] Vedi, in questo senso, le conclusioni dell'Avvocato Generale Niilo Jääskinen presentate il 25 giugno 2013.

[8] Vedi Corte di Giustizia dell'Unione europea, sent. 8 aprile 2014 (C-293/12 e C-594/12), con primo commento di R. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine*?, in http://www.penalecontemporaneo.it/upload/1398628841FLOR_2014.pdf, a cui si rinvia per gli ulteriori riferimenti bibliografici. Cfr. anche E. COLOMBO, Data retention e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della Direttiva 2006/24/CE, in Cass. pen., 7/8, 2014, 2705 e ss.

[9] Si fa riferimento alle concrete iniziative europee. In questa sede basti il rinvio a: http://ec.europa.eu/justice/data-protection/index_en.htm

[10] Per una descrizione dei fatti all'origine della sentenza si veda R. FLOR, *Dalla data retention al diritto all'oblio,* cit.

applicazione degli artt. 12, lett. b), e 14, co. 1, lett. a), della direttiva 95/46, possono ordinare al gestore del servizio (Google) di cancellare, dall'elenco di risultati che appare a seguito di una ricerca, i *link* verso pagine *web* pubblicate da terzi (nel caso di specie in una testata giornalistica *online*) e contenenti informazioni relative a una persona. Il fornitore del servizio è obbligato, inoltre, a sopprimere gli stessi *link* anche nel caso in cui il nome o le informazioni non vengano previamente o simultaneamente cancellati dalle pagine *web* del quotidiano, eventualmente quando la loro pubblicazione sia altresì di per sé lecita. Sulla base dell'interpretazione di tali prescrizioni, dettate dall'art. 6, co. 1, lett. da c) a e), direttiva 95/46, un trattamento di dati inizialmente lecito potrebbe divenire, con il tempo, incompatibile con la direttiva, qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura, in particolare, nel caso in cui i dati risultino inadeguati, non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità e al medesimo tempo trascorso. E'agevole notare che, secondo la Corte, i diritti fondamentali di cui agli artt. 7 e 8 della Carta prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico degli utenti a trovare l'informazione in occasione di una ricerca *online* relativa ad una persona determinata. Ferme restando, secondo i Giudici, le eccezioni legate, ad esempio, al ruolo ricoperto da tale persona nella vita pubblica, che potrebbe giustificare la prevalenza dell'interesse degli utenti ad avere accesso all'informazione[11].

Le motivazioni della sentenza muovono, anzitutto, dalle definizioni di "trattamento" di dati e di "responsabile del trattamento" (o, meglio, "titolare del trattamento"), così come previste dalla direttiva.

La prima, ex art. 2, lett. b), è estremamente ampia e fa riferimento a qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione.

La Corte ha già avuto modo di affrontare la questione e ha concluso che l'operazione consistente nel far comparire su una pagina Internet dati personali deve essere considerata un «trattamento»[12].

Nel c.d. caso Google/Spagna sono presenti anche informazioni riguardanti persone fisiche identificate o identificabili, e dunque «dati personali» . Di conseguenza l'uso della rete e di un motore di ricerca comporta che il gestore di questo ultimo «raccoglie» , «estrae», «registra» e «organizza» tramite i suoi programmi di indicizzazione, «conserva» e, eventualmente, «comunica» e «mette a disposizione» dei propri utenti tali dati e informazioni, essendo indifferente che essi non vengano modificati dal motore di ricerca o vengano elaborati in modo automatizzato dai softwares o dagli applicativi.

Quanto alla questione se il gestore di un motore di ricerca debba essere considerato «responsabile del trattamento» dei dati personali appare decisivo il fatto che egli stesso a determina le finalità e gli strumenti della sua attività e, dunque, del trattamento di dati

[11] Per quanto riguarda la situazione italiana *in subiecta materia* basti il rinvio al recente provvedimento del Garante Privacy, 10 luglio 2014, n. 353.

[12] Si veda caso Lindqvist (C-101/01, EU:C:2003:596, punto 25)

personali che effettua. Pertanto può essere considerato senza dubbio un «responsabile» (o, meglio, titolare - *controller*) ex art. 2, lett. d), della direttiva.

Il trattamento di dati personali effettuato nell'ambito dell'attività di un motore di ricerca, ad ogni modo, si distingue nettamente da quello effettuato dai gestori di siti o dagli editori di *web-sites* o testate giornalistiche *online.*

Il primo, infatti, scansiona e organizza le informazioni tramite procedimenti di indicizzazione, rinviando a pagine *web* o a contenuti presenti nella rete. Si tratta di un'attività che può essere oggetto di limitazioni da parte dei gestori dei siti, dei *social media* o dei *social network*s nonché, in alcuni casi, da parte degli utenti stessi, i quali possono richiedere di essere esclusi in tutto o in parte dagli indici automatici.

Rimane però fermo un dato oggettivo, ossia che le finalità e gli strumenti anche di tale trattamento sono determinati dal gestore del motore di ricerca.

In sintesi, dunque, ex art. 2, lett. b) e d) della direttiva 95/46, da un lato, l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», se tali informazioni contengano dati personali, e, dall'altro lato, il gestore del motore di ricerca deve essere considerato «responsabile» ("titolare") del trattamento.

Ne consegue logicamente che tale trattamento di dati effettuato per le esigenze del funzionamento del motore di ricerca non è sottratto agli obblighi e alle garanzie previsti dalla direttiva per la tutela delle libertà e dei diritti fondamentali delle persone fisiche, in particolare del diritto al rispetto della vita privata e dei dati personali (ex artt. 7 e 8 della Carta)[13].

Per quanto riguarda il trattamento di dati effettuato da Google, l'art. 7, lett. f), della direttiva 95/46, richiede di operare un bilanciamento di interessi fra i diritti coinvolti, consendo il trattamento dei dati se risulta essere necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del terzo o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, la quale può opporsi per motivi legittimi al trattamento dei dati che la riguardano, ex art. 14, co. 1, lett. a) della direttiva.

Tale diritto può essere esercitato direttamente nei confronti del titolare del trattamento, oppure attraverso il ricorso all'autorità di controllo o all'autorità giudiziaria (artt. 12, lett. b), e 14, co. 1, lett. a) della direttiva 95/46)

Considerata la potenziale gravità dell'ingerenza nell'area di "riservatezza" pertinente alla persona, il trattamento dei dati da parte del gestore di un motore di ricerca non può essere giustificato solo sulla base di interessi di natura economica.

E' vero, come affermano i Giudici, che la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a

[13] Questo ultimo prevede che i dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica, e che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente. In tal senso gli Stati membri devono garantire a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento, a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non sia conforme alle disposizioni della direttiva.

quest'ultima. E' però altresì vero che sia la direttiva, che la Carta esigono che venga effettuato un corretto bilanciamento tra tale interesse e i diritti fondamentali della persona di cui agli artt. 7 e 8 della stessa Carta.

Il trattamento dei dati effettuato dal gestore del motore di ricerca si aggiunge a quello effettuato dagli editori di siti web, distinguendosi allo stesso tempo.

Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli artt. 12, lett. b), e 14, co. 1, lett. a), della direttiva contro il gestore del motore di ricerca, ma non contro l'editore della pagina web, che potrebbe aver trattato i dati «esclusivamente a scopi giornalistici».

Sulla base di queste principali argomentazioni i Giudici hanno ritenuto che nel c.d. caso Google/Spagna non sussistessero ragioni per affermare come preponderante l'interesse del pubblico ad avere accesso, nel contesto di una ricerca *online*, alle informazioni personali, ritenendo prevalenti i diritti di cui agli artt. 7 e 8 della Carta, anche rispetto all'interesse economico del gestore del motore di ricerca, purchè vi sia una verifica inerente al diritto dell'interessato, che potrebbe essere sacrificato nel caso in cui sussitano ragioni particolari (come il ruolo ricoperto nella vita pubblica) che giustifichino l'ingerenza nei suoi diritti fondamentali per la sussistenza di un interesse preponderante del pubblico ad ottenere l'informazione.

3. La sentenza della Corte di Giustizia sulla c.d. *data retention*: un importante passo per il rafforzamento del diritto alla riservatezza. Ma con quali effetti per il sistema di giustizia penale?

In questo già articolato contesto la sentenza della Corte di Giustizia sulla c.d. *data retention* ha notevolmente complicato la situazione[14].

I Giudici, infatti, hanno invalidato la direttiva 2006/24, in quanto non compatibile con i limiti imposti dal rispetto del principio di proporzionalità, alla luce degli artt. 7, 8 e 52, par. 1, della Carta.

Tale direttiva richiedeva l'applicazione degli obblighi di conservazione a tutti i dati di traffico connessi a qualsiasi mezzo comunicativo. Questi obblighi riguardavano, dunque, l'archiviazione di dati relativi, in modo generalizzato, a tutti gli utenti e a tutti i mezzi di comunicazione elettronica, così come a tutte le modalità di traffico delle informazioni (via telefono, Internet, e-mail ecc.) senza differenziazioni, limiti o eccezioni rispetto all'obiettivo di contrastare la criminalità grave. Inoltre, tale archiviazione aveva ad oggetto dati di persone che, nemmeno indirettamente, si trovavano nella situazione di dare adito a procedimenti penali o di essere collegate, anche solo in modo remoto, a reati gravi, anche in situazioni in cui non sussistevano prove che la loro condotta potesse in qualche modo far sospettare un loro coinvolgimento. Inoltre essa non prevedeva alcuna eccezione, con la conseguenza che si trovava ad essere applicata anche alle persone le cui comunicazioni erano soggette, in base alle norme di diritto nazionale, all'obbligo del segreto professionale.

[14] Corte di Giustizia dell'Unione europea, sent. 8 aprile 2014 (C-293/12 and C-594/12), con commento di R. FLOR, *La corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 28 aprile 2014, 1-16, a cui si rinvia per l'approfondimento delle argomentazioni della Corte. Cfr., con riferimento agli effetti sia a livello europeo che nel sistema tedesco, S. NELLES, *Quo vadis Vorratsdatenspeicherung*?, Göttingen, 2014.

La direttiva non prevedeva nemmeno alcun rapporto tra i dati oggetto dell'obbligo di conservazione e una minaccia per la sicurezza pubblica. In particolare, tale obbligo non era limitato a: a) dati relativi a un determinato periodo di tempo e/o una particolare zona geografica e/o ad un cerchio di persone che potevano essere coinvolte, in un modo o nell'altro, in un crimine grave; b) a persone che potevano, per altri motivi, contribuire, grazie alla conservazione dei loro dati, alla prevenzione, accertamento e perseguimento di reati gravi.

La direttiva non prevedeva nemmeno alcun limite oggettivo, sostanziale o procedurale[15], per l'accesso ai dati da parte delle competenti autorità nazionali e per il successivo utilizzo a fini di prevenzione, accertamento [o nell'ambito di procedimenti penali] riguardanti reati che, in considerazione della portata e della invasività della interferenza con i diritti fondamentali di cui agli artt. 7 e 8 della Carta, fossero di una gravità tale da giustificare una limitazione a questi diritti. Al contrario, la direttiva faceva riferimento in modo generale, ex art. 1, par. 1, a «reati gravi» come «definiti dagli Stati membri», e non prevedeva che l'accesso ai dati avvenisse dopo l'esame di un giudice o di una autorità amministrativa indipendente, la cui decisione potesse, a seguito di una richiesta motivata presentata nel quadro delle procedure di prevenzione o accertamento di gravi reati, o nell'ambito di procedimenti penali, limitare l'accesso ai dati e il loro utilizzo a quanto fosse strettamente necessario ai fini del raggiungimento dell'obiettivo perseguito.

Per quanto riguarda il periodo di archiviazione dei dati, la direttiva faceva riferimento ad un lasso di tempo minimo (6 mesi) e massimo (24 mesi) senza distinguere le categorie di dati e la loro possibile utilità per il raggiungimento degli obiettivi perseguiti, ovvero in accordo con le persone coinvolte. Inoltre, il "periodo finestra" non era basato su criteri oggettivi al fine di assicurare che fosse limitato alla stretta necessità. Ne consegue che l'interferenza con i diritti fondamentali in esame avveniva senza limiti o regole precise.

Con riferimento alla sicurezza ed alla protezione dei dati oggetto dell'obbligo di archiviazione, la direttiva non prevedeva misure di garanzia sufficienti – come richieste, invece, dagli artt. 7 e 8 della Carta – in specie contro il rischio di abusi, accesso illegale o uso non autorizzato, nonchè in relazione alla molteplicità e diversità di dati che dovevano essere archiviati, alla natura dei medesimi ed ai rischi connessi alla loro integrità, confidenzialità e genuinità. La direttiva, inoltre, non prevedeva l'obbligo per gli Stati membri di disciplinare elevati standard di sicurezza, permettendo in tal modo ai *providers* di poter seguire criteri di mera economicità per assicurare la protezione delle informazioni[16]. Infine, la direttiva non richiedeva che i dati in questione dovessero essere conservati all'interno dell'Unione europea, con la conseguenza che non era possibile ritenere che il controllo, espressamente richiesto dall'art. 8, par. 3 della Carta,

[15] L'art. 4 della direttiva, infatti, lascia agli Stati membri il compito di definire le regole procedurali da seguire e i requisiti sostanziali per garantire l'accesso e la comunicazione dei dati.

[16] Il c.d. "criterio di economicità" era già stato evidenziato, in senso critico, dalla Corte costituzionale tedesca nella citata sentenza del 2 marzo 2010 sulla *data retention* (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), *on-line* in http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html Per un primo commento in italiano si consenta il rinvio a R. FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul* data retention, in *Ciberspazio e diritto*, 11, 2 , 2010 , 359-392. Nella letteratura tedesca vedi S. NELLES, *Quo vadis Vorratsdatenspeicherung*?, cit., 265 e ss.

da parte di un'autorità indipendente in conformità con le esigenze di tutela e sicurezza dei dati, fosse pienamente garantito.

Leggendo a contrario questa sentenza è possibile ricavare alcune linee guida per una riforma della normativa sulla c.d. *data retention*.

Ferme le delicate questioni sui limiti temporali della conservazione dei dati e sulle procedure di accesso e di acquisizione delle informazioni, le criticità principali riguardano, *in primis*, l'individuazione dei "gravi" reati "presupposto", nonché la definizione dei presupposti oggettivi che possano giustificare la *data retention.* In secondo luogo, la valutazione sull'esistenza di un *fumus commissi delicti* dovrebbe essere lasciata ad un organismo indipendente (giudice) attraverso la previsione di una procedura snella e "tempestiva", che consenta comunque un accertamento concreto sulla sussistenza del reato "presupposto", basato su elementi indiziari (provvedimento motivato dell'autorità giudiziaria su richiesta del pubblico ministero, anche su istanza del difensore dell'imputato), che può pervenire *ex post*, in un lasso di tempo comunqe breve, esclusivamente in ipotesi di urgenza (ad esempio quando sussistono elementi oggettivi e concordanti relativi alla preparazione di attentati terroristici), purchè vi sia una definizione: a) di un elevato livello delle "misure di sicurezza" da adottare e delle procedure da seguire per la conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento; b) di apposite sanzioni di inutilizzabilità del materiale probatorio acquisito in modo illecito o in caso di mancato rispetto del "principio di necessità" nel trattamento dei dati (ad esempio quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato o le persone a lui collegate solo in caso di indispensabilità).

Nel caso in cui le norme interne dei singoli Stati, come nel caso italiano, non rispettino gli standard ricavabili dalla sentenza della Corte, esse dovrebbero essere disapplicate per contrasto con il diritto europeo.

La soluzione più immediata, ma purtroppo ad effetto "locale", vede come protagonista il legislatore nazionale, il quale dovrebbe intervenire ed adattare l'attuale disciplina agli standards elaborati dalla Corte di Giustizia.

Sarebbe però maggiormente auspicabile un intervento del legislatore europeo, nell'ambito di una più ampia politica criminale dell'Unione. La stessa individuazione dei fenomeni criminali gravi e di natura transnazionale, nonché la conseguente definizione dei "reati presupposto", potrebbe trovare una base legale nell'art. 83, par. 1, del Trattato sul funzionamento dell'Unione europea (TFUE).

Il *valore aggiunto* riguarda, da un lato, l'efficacia, per la forza vincolante delle fonti per gli Stati membri; dall'altro lato le *garanzie,* che devono circondare la produzione di norme penali (legittimazione democratica e trasparenza del procedimento legislativo, controllabilita` politica, da parte dei Parlamenti nazionali durante la fase « ascendente » dei fondamentali principi di sussidiarieta` europea e di proporzionalita`, ex art. 5 TUE e Protocollo applicativo n. 2 allegato al TFUE, piena controllabilita` giudiziaria di tali presupposti da parte della Corte di Giustizia ed, indirettamente, delle giurisdizioni nazionali nella fase applicativa).

L'epocale sentenza della Corte di Giustizia, di cui si condivide l'iter argomentativo e motivazionale, che fonda le proprie basi nel percorso già intrapreso da numerose Corti

costituzionali europee [17], si scontra con la complessità dell'attuale società dell'informazione, governata dalla inarrestabile rivoluzione informatica e dalla esasperata velocità evolutiva delle tecnologie, che hanno trasformato i dati e le informazioni in "beni immateriali" di inestimabile valore.

Nell'attuale assetto sociale ed economico il ricorso a strumenti investigativi a "contenuto tecnologico" e alla *data retention* risulta indispensabile, per prevenire e per accertare gravi reati lesivi di importanti beni giuridici[18].

Nella delicata operazione di bilanciamento fre le contrapposte esigenze di tutela, il c.d. "diritto all'oblio", afferente alle prerogative della sfera di riservatezza della peronsa, deve essere considerato proprio rispetto all'interesse generale dell'accertamento e prevenzione di gravi reati.

I principi espressi dalle sentenze della Corte di Giustizia sui casi c.d. data retention e Google/Spagna, devono essere letti congiuntamente per tentare di elaborare una griglia di standards minimi per consentire tale giudizio di bilanciamento e per definire i contorni dei possibili limiti al diritto del soggetto interessato di ottenere la cancellazione dei dati e delle informazioni che lo riguardano anche da motori di ricerca.

4. Verso una definizione del "diritto all'oblio"

4.1. Il diritto all'oblio nelle conclusioni dell'Avvocato Generale

La ricostruzione del "diritto all'oblio" effettuata dalla Corte di Giustizia nella sentenza Google/Spagna in parte contrasta con le conclusioni dell'avvocato generale, il quale ha affermato, sulla base di specifiche argomentazioni, che non possa ritenersi pacifico poter ricavare dalle norme della direttiva 95/46 (direttiva), intepretate alla luce delle disposizioni dalla Carta, un diritto "generalizzato" all'oblio.[19]

Secondo l'avvocato generale, infatti, *i diritti alla rettifica, alla cancellazione, al congelamento e all'opposizione previsti nella direttiva non corrispondano al «diritto all'oblio» della persona interessata*

In particolare la direttiva non prevederebbe un diritto generale di questo che possa permettere al soggetto interessato di limitare o di impedire la diffusione di dati personali che egli consideri compromettenti o contrari ai propri interessi.

I criteri da applicare dovrebbero invece essere individuati nello scopo del trattamento e negli interessi da questo tutelati, bilanciati con quelli della persona interessata, e non invece con le preferenze di quest'ultima. Pertanto, una preferenza soggettiva non

[17] Vedi R. FLOR, *La Corte di Giustizia*, cit., 1-16.

[18] Gli stessi Stati membri, in generale, hanno affermato che la conservazione dei dati è «quanto meno utile, e in alcuni casi indispensabile, per prevenire e contrastare la criminalità, compresa la protezione delle vittime e l'assoluzione degli imputati innocenti». La Repubblica ceca, ad esempio, ha considerato la conservazione dei dati «assolutamente indispensabile in un gran numero di casi»; la Slovenia ha indicato che l'assenza di dati conservati «paralizzerebbe l'attività delle agenzie di contrasto»; l'Ungheria ha affermato che era «indispensabile nelle attività ordinarie [delle agenzie di contrasto]»; il Regno Unito ha descritto la disponibilità di dati relativi al traffico come «assolutamente essenziale … per condurre indagini riguardanti il terrorismo e i reati gravi». Vedi in questo senso il rapporto della Commissione europea relativo alla "Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24)", COM(2011) 225 definitivo, 25, nota 105.

[19] Vedi, in questo senso, le conclusioni dell'Avvocato Generale Niilo Jääskinen presentate il 25 giugno 2013.

dovrebbe costituire un motivo preminente e legittimo ai sensi dell'articolo 14, lett. a), della direttiva 95/46.

Anche se il gestore del motore di ricerca è riconducibile alla categoria dei «responsabili del trattamento» (o, meglio, titolare/*controller*), la persona interessata non avrebbe in ogni caso un «diritto all'oblio» assoluto da far valere.

La sentenza della Corte affronta la questione del bilanciamento soprattutto rispetto alla tutela della libertà di espressione e di impresa, seguendo la linea interpretativa della Corte europea dei diritti dell'uomo, la quale ha già dichiarato, nella sentenza Aleksey Ovchinnikov[20] , che «in alcuni casi può essere giustificato limitare la riproduzione di informazioni già divenute di pubblico dominio, ad esempio al fine di impedire un'ulteriore diffusione dei dettagli della vita privata di una persona estranea a qualsiasi dibattito politico o pubblico su un argomento di importanza generale». Pertanto, in linea di principio, il diritto fondamentale alla protezione della vita privata può essere invocato anche se le informazioni di cui trattasi sono già di pubblico dominio.

Non ha torto l'Avvocato Genereale qunado sostiene che il problema della protezione dei dati si è posto, in questo caso, solo quando un utente ha inseritio nome e cognome della persona interessata nel motore di ricerca ottenendo un link verso le pagine web di un giornale in cui compaiono gli articoli contestati. L'utente ha però *esercitato attivamente il proprio diritto ad ottenere informazioni relative alla persona interessata provenienti da fonti pubbliche* per motivi che possono essere fra i più disparati. Cercare informazioni tramite motori di ricerca costituisce, nell'attuale contesto sociale, forse lo strumento più importante per esercitare tale diritto fondamentale.

Partendo da questa prospettiva, e considerando il legittimo diritto di impresa del fornitore dei servizi in Internet e del gestore del motore di ricerca, ossia quello di organizzare e indicizzare i risultati delle ricerche degli utenti, riconoscere valore predominante al diritto all'oblio vorrebbe dire sacrificare la libertà di espressione e di informazione, che potrebbero essere compromesse ulteriormente se la valutazione, caso per caso, fosse lasciata solo alla decisione degli stessi fornitori di servizi.

In tale contesto, è condivisibile l'osservazione dell'Avvocato Generale, quando avverte che le «procedure di notifica e rimozione» di cui alla direttiva 2000/31 sul commercio elettronico si riferiscono a "contenuti illeciti, mentre il presente caso verte su una richiesta di soppressione di informazioni legittime e legali entrate nella sfera pubblica".

4.2 Il diritto all'oblio nella proposta di regolamento europeo concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)

Il c.d. diritto all'oblio è espressamente disciplinato dall'art. 17 della Proposta della Commissione per un regolamento generale sulla protezione dei dati personali[21] .

In estrema sintesi tale disposizione prevede il diritto all'oblio e alla cancellazione[22], rafforzando il diritto alla cancellazione di cui all'art. 12, lett. b) direttiva 95/46, nonché

[20] Aleksey Ovchinnikov v. Russia, n. 24061/04, 16 dicembre 2010.

[21] Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 def., 25 gennaio 2012.

l'obbligo per il responsabile (titolare) del trattamento che abbia divulgato dati personali di informare i terzi della richiesta dell'interessato di cancellare tutti i link verso tali dati, le loro copie o riproduzioni. La disposizione prevede inoltre il diritto di limitare il trattamento in determinati casi, evitando l'ambiguo termine di "blocco dei dati". In particolare, l'interessato deve avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o trattati, quando abbia ritirato il consenso o si sia opposto al trattamento o quando questo ultimo non sia conforme alle disposizioni del regolamento. Tuttavia, occorre consentire l'ulteriore conservazione dei dati qualora sia necessario per finalità storiche, statistiche e di ricerca scientifica, per motivi di interesse pubblico nel settore della sanità pubblica, per l'esercizio del diritto alla libertà di

[22] Si riporta di seguito il testo dell'art. 17. "L'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l'interessato era un minore, se sussiste uno dei motivi seguenti: a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si fonda il trattamento, di cui all'articolo 6, paragrafo 1, lettera a), oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattare i dati; c) l'interessato si oppone al trattamento di dati personali ai sensi dell'articolo 19; d) il trattamento dei dati non è conforme al presente regolamento per altri motivi. 2. Quando ha reso pubblici dati personali, il responsabile del trattamento di cui al paragrafo 1 prende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione. 3. Il responsabile del trattamento provvede senza ritardo alla cancellazione, a meno che conservare i dati personali non sia necessario: (a) per l'esercizio del diritto alla libertà di espressione in conformità dell'articolo 80; (b) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 81; (c) per finalità storiche, statistiche e di ricerca scientifica in conformità dell'articolo 83; (d) per adempiere un obbligo legale di conservazione di dati personali previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento; il diritto dello Stato membro deve perseguire un obiettivo di interesse pubblico, rispettare il contenuto essenziale del diritto alla protezione dei dati personali ed essere proporzionato all'obiettivo legittimo; (e) nei casi di cui al paragrafo 4. 4. Invece di provvedere alla cancellazione, il responsabile del trattamento limita il trattamento dei dati personali: a) quando l'interessato ne contesta l'esattezza, per il periodo necessario ad effettuare le opportune verifiche; b) quando, benché non ne abbia più bisogno per l'esercizio dei suoi compiti, i dati devono essere conservati a fini probatori; c) quando il trattamento è illecito e l'interessato si oppone alla loro cancellazione e chiede invece che ne sia limitato l'utilizzo; d) quando l'interessato chiede di trasmettere i dati personali a un altro sistema di trattamento automatizzato, in conformità dell'articolo 18, paragrafo 2. 5. I dati personali di cui al paragrafo 4 possono essere trattati, salvo che per la conservazione, soltanto a fini probatori o con il consenso dell'interessato oppure per tutelare i diritti di un'altra persona fisica o giuridica o per un obiettivo di pubblico interesse. 6. Quando il trattamento dei dati personali è limitato a norma del paragrafo 4, il responsabile del trattamento informa l'interessato prima di eliminare la limitazione al trattamento. 7. Il responsabile del trattamento predispone i meccanismi per assicurare il rispetto dei termini fissati per la cancellazione dei dati personali e/o per un esame periodico della necessità di conservare tali dati. 8. Quando provvede alla cancellazione, il responsabile del trattamento si astiene da altri trattamenti di tali dati personali. 9. Alla Commissione è conferito il potere di adottare atti delegati in conformità all'articolo 86 al fine di precisare: a) i criteri e i requisiti per l'applicazione del paragrafo 1 per specifici settori e situazioni di trattamento dei dati; b) le condizioni per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico, come previsto al paragrafo 2; c) i criteri e le condizioni per limitare il trattamento dei dati personali, di cui al paragrafo 4".

espressione, ove richiesto per legge o quando sia giustificata una limitazione del trattamento dei dati anziché una loro cancellazione.

Per garantire tale informazione, è necessario che il responsabile (titolare) del trattamento prenda tutte le misure ragionevoli, anche di natura tecnica, in relazione ai dati della cui pubblicazione è responsabile, anche se ha autorizzato un terzo a pubblicarli.

Anche nei casi in cui i dati personali possano essere lecitamente trattati per proteggere interessi vitali dell'interessato, oppure per motivi di pubblico interesse, nell'esercizio di pubblici poteri o per il legittimo interesse di un responsabile (titolare) del trattamento, l'interessato deve comunque avere il diritto di opporsi al trattamento dei dati che lo riguardano.

La proposta di regolamento, però, prevede specifiche limitazioni al diritto all'oblio e alla cancellazione dei dati, fornendo una base giuridica per il bilanciamento fra contrapposte esigenze, ancorata al rispetto del principio di legalità. L'art. 21, infatti, dispone che l'Unione o gli Stati membri possono limitare, mediante misure legislative, la portata di tale diritto qualora la limitazione costituisca una misura necessaria e proporzionata in una società democratica per salvaguardare: a) la pubblica sicurezza; b) le attività volte a prevenire, indagare, accertare e perseguire reati; c) altri interessi pubblici dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, e la stabilità e l'integrità del mercato; d) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; e) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lett. a), b), c), e d); f) la tutela dell'interessato o dei diritti e delle libertà altrui.

La questione più delicata riguarda l'individuazione dell'organo o del soggetto deputato al giudizio di bilanciamento fra le diverse esigenze, da un lato, di tutela della riservatezza e, dall'altro lato, di giustizia penale o per la tutela della sicurezza pubblica o, ancora, per la protezione della libertà di espressione.

L'art. 12 della proposta di regolamento fa incombere in prima battuta sul responsabile (titolare) del trattamento l'obbligo di stabilire le procedure per l'esercizio dei diritti dell'interessato, fra i quali quelli di cui all'art. 17, che devono comprendere l'informazione a tale soggetto, tempestivamente e al più tardi entro un mese – termine prorogabile in casi specifici (se più interessati esercitano i loro diritti e la loro cooperazione è necessaria in misura ragionevole per evitare un impiego di risorse inutile e sproporzionato al responsabile del trattamento dal ricevimento della richiesta) - se è stata adottata un'azione. Se il responsabile (titolare) rifiuta di ottemperare alla richiesta dell'interessato, egli deve informarlo dei motivi e delle possibilità di proporre reclamo all'autorità di controllo e anche ricorso giurisdizionale.

E' noto che nella maggior parte dei casi il fornitore di servizi è un soggetto privato che esercita la libertà di impresa. Egli dovrebbe dimostrare, in caso di rifiuto, non solo che i suoi legittimi interessi possono prevalere sull'interesse o sui diritti e sulle libertà fondamentali dell'interessato, ma anche che la richiesta, nel settore che qui interessa, non possa essere accolta per le esigenze legate alle attività volte a prevenire, indagare, accertare e perseguire reati.

La proposta di regolamento, però, non individua espressamente un nucleo di reati gravi, che possano giustificare un'invasione nella sfera di riservatezza dell'individuo o, quantomeno, la necessità di proteggere beni giuridici di predominante importanza.

Inoltre, il fornitore di servizi coinvolto attivamente in attività di indagine svolge un ruolo di carattere "pubblico", che comporta in molti casi il riserbo sulla natura del coinvolgimento o sull'attività che è "delegato" a svolgere per gli organi investigativi.

Egli sarà dunque portato a rifiutare la cancellazione dei dati o il pieno esercizio del diritto all'oblio, lasciando all'autorità di controllo o all'autorità giudiziaria giudicare su eventuali reclami.

La proposta di regolamento, però, prevede, ex art. 79, specifiche sanzioni amministrative nel caso in cui il responsabile (titolare) non rispetti il diritto all'oblio o alla cancellazione, ometta di predisporre meccanismi che garantiscano il rispetto dei termini o non prenda tutte le misure necessarie per informare i terzi della richiesta dell'interessato di cancellare tutti i link verso i dati personali, copiare tali dati o riprodurli, in violazione dell'art. 17, salve le ulteriori sanzioni, che potrebbero avere altresì natura penale, previste dagli Stati membri, ex art. 78 della stessa proposta.

A ciò si aggiungono gli obblighi generali previsti dall'art. 22 della proposta, fra cui quelli inerenti alla sicurezza dei dati, disciplinati dal successivo art. 30.

In conclusione, il diritto all'oblio definito dalla nuova proposta non è (naturalmente) di natura assoluta e omnicomprensivo dei diritti riconosciuti al soggetto interessato.

5. Verso una definizione "integrata" del diritto all'oblio e possibili linee guida per il bilanciamento con le esigenze proprie del sistema di giustizia penale

A questo punto, e ai fini del presente lavoro, non rimane che affrontare la questione relativa ai rapporti fra diritto all'oblio ed esigenze di perseguire, accertare o prevenire gravi reati, che presuppone la lettura integrata fra le sentenze della Corte di Giustizia sulla *data retention* e sul caso Google/Spagna.

In prospettiva *de jure condendo*, considerando la proposta di regolamento europeo, nella sua attuale formulazione, si potrebbe delimitare il c.d. diritto all'oblio, anche nell'ottica di una auspicabile disciplina degli obblighi di archiviazione dei dati di traffico telefonico e telematico.

Dovrebbe però essere prevista la possibilità di cancellare o rimuovere i dati personali, su richiesta del soggetto interessato, in particolare dai motori di ricerca, dopo un periodo – finestra determinato, in cui eventualmente tali informazioni dovrebbero essere rese non accessibili al pubblico o alle persone non autorizzate.

In tal caso il legislatore europeo, alla luce delle citate sentenze della Corte, dovrebbe osservare le linee guida ricavabili dalla decisione sulla c.d. *data retention* e predisporre un "sistema di obblighi integrato", che preveda: limiti temporali alla conservazione dei dati; procedure di accesso e di acquisizione delle informazioni; l'individuazione dei "gravi" reati "presupposto", nonché la definizione dei presupposti oggettivi che possano giustificare la *data retention; che* la valutazione sull'esistenza dei presupposti sia lasciata ad un organismo indipendente (giudice) attraverso la previsione di una procedura snella e "tempestiva", purchè vi sia una definizione a) di un elevato livello delle "misure di sicurezza" da adottare e delle procedure da seguire per la conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento; b) di apposite sanzioni di inutilizzabilità del materiale

probatorio acquisito in modo illecito o in caso di mancato rispetto del "principio di necessità" nel trattamento dei dati.

A questi presupposti dovrebbero aggiungersi gli obblighi di rendere inaccessibili i dati, su richiesta del soggetto interessato. In tal caso si tratterebbe di un diritto all'oblio bifasico. In una prima fase l'interessato otterrebbe l'effetto di non rendere accessibili le informazioni (ad esempio tramite motori di ricerca o i siti che le contengono), le quali però, sul piano tecnico, rimarrebbero a disposizione del fornitore del servizio – se il soggetto destinatario dell'obbligo è riconducibile a questa categoria - per un periodo limitato, utile e necessario per il perseguimento, l'accertamento o la prevenzione di gravi reati. In tal caso sarebbe possibile il coordinamento fra la proposta di regolamento europeo, in particolare dell'art. 21, con una futura e auspicabile disciplina europea in materia di *data retention*.

In una seconda fase, ossia trascorso il periodo previsto da tale ultima disciplina, il fornitore del servizio potrebbe procedere alla cancellazione del dato, salve le ulteriori esigenze di proroga della conservazione nel caso in cui il soggetto interessato sia divenuto indagato o imputato in un procedimento penale. In tale ultima situazione potrebbe trovare piena applicazione una disposizione quale quella di cui all'art. 21 della proposta di regolamento. La qualità di indagato o imputato, infatti, giustificherebbe la conservazione di dati anche con riferimento ai reati non inclusi in un'ipotetica lista di incriminazioni presupposto di una certa gravità.

Per quanto riguarda gli aspetti "procedurali", un primo modello potrebbe essere ricavato dalla direttiva e-commerce e basarsi su un procedimento ingiunzionale connotato da un atto qualificato di un organismo indipendente (un giudice, anche eventualmente su segnalazione o su richiesta della persona fisica o dell'autorità garante), in modo da consentire di effettuare il bilanciamento fra le contrapposte esigenze di tutela e di perseguimento di interessi generali collettivi, che non può essere lasciato all'apprezzamento "soggettivo" del singolo provider [23]. Tale "modello" troverebbe conferma sia nella sentenza della Corte sulla *data retention* sia in quella sul caso Google/Spagna[24].

La "gravità potenziale" dell' ingerenza nei diritti fondamentali verrebbe via via affievolita proprio in base alla rilevanza dei contro interessi e dei diritti che necessiterebbero di tutela quantomeno paritaria.

A ciò deve aggiungersi che a favore della non cancellazione possono sussistere, in primo luogo, anche ragioni statali tipiche di natura paternalistica, ossia quando i dati

[23] Si vedano i rilievi critici espressi da R. Flor, La Corte di Giustizia, cit.

[24] Vedi punto 82 della sentenza: «L'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di applicazione degli artt.12, lett. b), e 14, co. 1, lett. a), della direttiva 95/46, da effettuarsi allorché ricevono una domanda quale quella oggetto del procedimento principale, possono ordinare al suddetto gestore di sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona, senza che un'ingiunzione in tal senso presupponga che tale nome e tali informazioni siano, con il pieno consenso dell'editore o su ingiunzione di una delle autorità sopra menzionate, previamente o simultaneamente cancellati dalla pagina web sulla quale sono stati pubblicati». Ex art. 28, par. 3 e 4 della direttiva, qualsiasi persona può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali, e che tale autorità dispone di poteri investigativi e di poteri effettivi di intervento che le consentono di ordinare in particolare il congelamento, la cancellazione o la distruzione di dati, oppure di vietare a titolo provvisorio o definitivo un trattamento.

sono raccolti ed archiviati nell'interesse del medesimo individuo e/o della collettività. In tal caso, pur potendo limitare l'accesso a queste informazioni, esse non dovrebbero essere completamente eliminate ma solamente, e eventualmente, oscurate (rectius rese accessibili solo a persone determinate, autorizzate o legittimate).

In secondo luogo, possono prevalere non solo interessi collettivi o generali, che portano beneficio all'intera comunità, come nel caso delle esigenze legate alla repressione e alla prevenzione dei reati, nonché alla raccolta della prova in formato digitale, che rispondo altresì all'esigenza di proteggere la sicurezza nazionale, ma anche, come ha affermato la Corte di Giustizia, la libertà di espressione e la libertà economica[25].

Fermo restando il diritto del soggetto interessato di ottenere, tramite l'ordine di un giudicie, la cancellazione di dati o informazioni che lo riguardano, che costituiscono gli "effetti" o il "pregiudizio" di un illecito già accertato (si pensi ai classici casi di diffamazione tramite *social networks*, blog o siti indicizzati dai motori di ricerca: in questo caso l'interesse principale della "vittima" è ottenere la rimozione della notizia diffamatoria dai risultati delle ricerche *online* e/o dai siti in cui si trova [26]). Analogamente, come è ricavabile dalle motivazioni della sentenza nel caso Google/Spagna, dovrebbe rimanere fermo il diritto all'oblio dell'autore di un reato che, scontata la pena, vede associato il proprio nome a fenomeni criminosi anche a distanza di molti anni, nel rispetto degli standard e dei meccanismi procedurali descritti dalla Corte stessa, eventualmente integrati con le ulteriori safeguards sopra riportate[27].

Ad ogni modo la domanda della persona interessata pressuppone l'incompatibilità con la direttiva 95/46 del trattamento, anche se questo inizialmente era da considerarsi lecito[28].

---

[25] In questo senso vedi P. Bernal, Internet Privacy Rights, Cambridge University Press, 2014, 199 e ss. E' utile tenere distinta la figura di un motore di ricerca rispetto a quella di siti-fonte o testate giornalistiche online. Il trattamento da parte dell'editore di una pagina web, infatti, potrebbe consistere nella pubblicazione di informazioni relative a una persona fisica, effettuata «esclusivamente a scopi giornalistici» . Ex art. 9 della direttiva 95/46, egli benificerebbe delle deroghe alle prescrizioni dettate da quest'ultima, mentre non integrerebbe tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca. Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli arti. 12, lett. b), e 14, co. 1, lett. a), della direttiva contro il suddetto gestore del motore di ricerca, ma non contro l'editore della pagina web.

[26] Si veda a titolo esemplificativo, fra alcuni dei più recenti casi italiani: Trib. Milano, ord. 24 marzo 2011. Si veda altresì la recente proposta di legge "Modifiche alla legge 8 febbraio 1948, n. 47, al codice penale e al codice di procedura penale in materia di diffamazione, di diffamazione con il mezzo della stampa o con altro mezzo di diffusione, di ingiuria e di condanna del querelante" (Atto Camera 925 – Atto Senato 1119), in particolare nella versione emendata a seguito della sentenza della Corte di Giustizia sul caso Google/Spagna: *«Art. 2-bis (Misure a tutela del soggetto diffamato o del soggetto leso nell'onore e nella reputazione) 1. Fermo restando il diritto di ottenere la rettifica o l'aggiornamento delle informazioni contenute nell'articolo ritenuto lesivo dei propri diritti, l'interessato può chiedere ai siti internet e ai motori di ricerca l'eliminazione dei contenuti diffamatori o dei dati personali trattati in violazione delle disposizioni di cui alla presente legge. 2. L'interessato, in caso di rifiuto o di omessa cancellazione dei dati, ai sensi dell'articolo 14 del decreto legislativo 9 aprile 2003, n. 70, può chiedere al giudice di ordinare ai siti internet e ai motori di ricerca la rimozione delle immagini e dei dati ovvero di inibirne l'ulteriore diffusione. 3. In caso di morte dell'interessato, le facoltà e i diritti di cui al comma 2 possono essere esercitati dagli eredi o dal convivente»*.

[27] Vedi *supra*, par. 2 e 3.

[28] Con il tempo, infatti, tale trattamento potrebbe non essere più necessario in rapporto alle finalità per le quali sono stati raccolti i dati, come nei casi in cui essi risultino inadeguati, o non siano più pertinenti, in rapporto proprio al tempo trascorso.

6. Conclusioni.

Nell'attuale assetto della società dell'informazione e di Internet non è possibile pensare di affrontare le sfide poste dalle nuove tecnologie senza poter sfruttare le loro potenzialità.

Per l'accertamento e la prevenzione di reati, infatti, l'accesso a dati e informazioni personali comporta spesso un "salto nel passato", per ricostruire trame comunicative, "spostamenti" *online* e, talvolta, fisici, sulla scorta di tecniche di localizzazione.

Il "monitoraggio" della rete e, dunque, anche dei risultati della ricerca tramite *search tools* e *web search engine* può risultare in molti casi un'attività indispensabile al fine non solo di raccogliere elementi indiziari o probatori, ma anche per individuare la fonte o il luogo "virtuale" specifico in cui sono "archiviati" i dati, oltre che per prevenire attività illecite e gravi reati.

La questione da porsi riguarda i limiti entro i quali può operare il legislatore (nazionale ed europeo) nella compromissione dei diritti fondamentali e nel prevedere gli standars su cui basare il delicato giudizio di bilanciamento con altri diritti fondamentali e con le esigenze di tutelare importanti interessi generali e collettivi, nel rispetto del principio di proporzione.

Al riguardo, l'art. 52 della Carta dei diritti fondamentali dell'Unione europea, identifica proprio nel principio di proporzione il criterio guida fondamentale, sia sul piano ermeneutico che su quello delle scelte politico normative del legislatore, delimitandone l'area di discrezionalità.

Sarebbe utopistico, infatti, credere che l'utente medio del nuovo millennio non utilizzi le opportunità offerte dalla evoluzione-rivoluzione informatica. Sarebbe altrettanto utopistico credere di contrastare forme di criminalità anche grave senza ricorrere alle stesse opportunità offerte dalla evoluzione-rivoluzione informatica.

Per queste ragioni le linee guida ricavabili dalla lettura sistematica delle sentenze della Corte di Giustizia sui casi Google/Spagna e *data retention* potrebbero costituire il primo ed importante mattone delle fondamenta su cui edificare i "parametri" certi per consentire il giudizio di bilanciamento fra le contrapposte esigenze di tutela, nonché di accertamento e prevenzione dei reati.

Laboratorio Permanente di Diritto Penale
Via Fontana, 28 – 20122 Milano (Italia)
C.F. 97664840150
Web: http://labdirpen.wix.com/diplap

Di.P.La.P. è un'associazione fondata da un gruppo di studiosi italiani di diritto e procedura penale per aggregare e rispondere alle istanze di rinnovamento e democratizzazione della ricerca e del dibattito penalistici. Valori costitutivi sono l'autonomia e l'indipendenza organizzativa e scientifica, la multidisciplinarietà, l'apertura al mondo extra-accademico e professionale, la solidarietà intergenerazionale.

Il volume raccoglie gli atti del I convegno nazionale del Laboratorio Permanente di Diritto Penale, che si è tenuto a Perugia il 19 settembre 2014, sul tema "La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet".

L'incontro è stato caratterizzato da un vivace dibattito sui temi più attuali che coinvolgono le complesse implicazioni fra il sistema penale e le nuove tecnologie in una prospettiva europea ed internazionale: la società dell'informazione, infatti, ha da tempo comportato dei cambiamenti epocali in ogni settore della vita umana, implicanti non solo molteplici opportunità di sviluppo "positivo", sul piano sociale, culturale ed economico.

Su questo fertile terreno fioriscono difatti anche nuovi fenomeni, modi e tipi di comportamenti di rilievo penale, e si aprono "altri" percorsi per commettere reati "tradizionali"; d'altro canto il mondo digitale si dimostra una fondamentale frontiera per la lotta alla criminalità moderna, offrendo innovativi strumenti e mezzi per la ricerca delle prove e, in generale, per il contrasto a vasti settori di illiceità penale.

I curatori

Daniela Falcinelli è ricercatrice a tempo determinato in diritto penale nell'Università di Perugia (sede di Terni, Narni), nonchè docente di diritto penale presso le Scuole forensi di diversi Consigli dell'Ordine degli Avvocati e corsi post lauream.

Roberto Flor è ricercatore confermato in diritto penale e professore aggregato di diritto penale, diritto penale dell'informatica ed International Criminal Law nell'Università di Verona.

Stefano Marcolini è ricercatore confermato in diritto processuale penale e professore aggregato in diritto penitenziario e diritto processuale penale nell'Università dell'Insubria (sede di Como).

DIPLAP Editor

2015